

REMARKS

Reconsideration and allowance are respectfully requested in light of the above amendments and the following remarks.

Claims 11-16 have been amended and claims 17-26 have been newly added. Claims 1-10 are canceled in favor of claims 17-26 to emphasize the patentable features of this invention. Claims 11-16, have been amended to clarify the claimed subject matter, to recite that the communication terminal identifier comprises a mobile terminal call number, and to place all claim elements in non-means-plus-function format. Support for the amendments to claims 11-16 and for new claims 17-26 is provided by *inter alia* Figs. 3, 14, and 29 and their accompanying descriptions in the specification. Support for claims 17-26 is provided by *inter alia* Figs. 5-10 and specification pages 20-36.

Regarding the language in the new claims, the first identifier is, e.g., a user ID number. The second identifier is of course the mobile communication terminal number. Referring to Fig. 4 for illustration purposes only, the first password and user ID are entered by the user at step 2, and database 310 stores the first password collated to the user ID. In step 9, the user ID is again provided to database 310 to ask for the second password and the call number. Thus, the database 310 stores the first password, the second password, and the call

number (second identifier) all collated to the user ID (first identifier). Thus, the wherein clause states "said first password, said second password and said mobile communication terminal number correspond to said first identifier in said database."

The office action rejected claims 1-16 under 35 USC 103 based on Foldare et al. (applied in the previous office action) and Ratayczak (newly applied). The Office has withdrawn reliance on Walker et al. To the extent these rejections are deemed applicable to amended claims 11-16 and new claims 17-26, the Applicants respectfully traverse.

Foladare discloses a system and method for allowing a parent to control the use of an ancillary credit or debit card issued to a child. The card issuer has a computer with a database containing account information and spending limits for the card. When the child presents the card, the merchant contacts a central computer for card authorization. The central computer then contacts the issuer computer, and the issuer computer checks the database. If the credit limit has been exceeded, the issuer's computer sends a method of contacting the parent to the central computer, and the central computer contacts the parent via, e.g., a two way pager or cellular telephone to query the parent whether to authorize the transaction, by increasing the spending limit of

the ancillary cardholder, or refuse it. The parent responds to the central computer, and the central computer forwards an approval/refusal to the merchant.

A problem with the Foladare system is that there is no use of passwords, much less a password known only to the parent that is used to verify the parent's identity when the approval/refusal is provided.

Ratayczak does not cure the deficiencies of Foladare.

Ratayczak teaches identification of a user or users using two individual connections between first and second communications devices C1 and C2 and an access determining device A (col. 1, lines 49-55), in order to transmit identification information of the user(s) (col. 3, line 11; col. 5, lines 34-35; and col. 6, lines 61-62) and plural code words to the determining device A for checking. Ratayczak does not teach the use of a mobile communication terminal number corresponding to a first identifier of a user stored in a member database. In Ratayczak, one or both of C1 and C2 receive access to system S (col. 3, lines 41-43). In the Fig. 2 embodiment of Ratayczak, there is no description of selection of C2 to send the second codeword to device A based on any identification information of the user. In the Fig. 4 embodiment of Ratayczak, another codeword is sent from device A to C1 (col. 5, lines 42-43) and then from C1 to C2 (col.

5, lines 54-56), and then from C2 to access device A (col. 5, lines 60-62) to enable one or both of C1 and C2 to gain access to System S.

Ratayczak provides no suggestion or motivation to modify Foladare given that Ratayczak is a completely different type of system from Foladare because in Ratayczak there is no transmission from device A to C2. There is no need for such transmission because C1 and C2 work cooperatively with each other to provide the two or more code words to gain access to system S. Further, in Foladare, the method of contacting the parent is independent of anything provided to the central computer by the child because otherwise someone besides the parent could provide the approval.

Ratayczak's failure to disclose a system wherein device A contacts C2 renders it very different in concept from Foladare, and thus, there would have been no reason for one skilled in the art to look to Ratayczak for a modification of Foladare to use passwords. Accordingly, there is a lack of motivation to combine the references as asserted in the office action.

Moreover, the office action does not make any specific assertion of how Foladare's system could be modified by the teachings of Ratayczak to achieve the claimed structure and method.

Further, even if the teachings of Foladare and Ratayczak were combined, it appears that the office action is in error in alleging that Ratayczak teaches authentication using two sets of identifiers and passwords communicated through two independent and separate channels (office action, page 4, second full paragraph), because Ratayczak lacks a teaching of second identification information of the user associated with the second password and because Ratayczak does not call for connection to the mobile terminal of the user by using the second identifier of the user (mobile terminal number) and for the second password of the user to be sent by the connected mobile communication terminal. Moreover, as noted above, Ratayczak does not teach the use of a mobile communication terminal number corresponding to an identifier of a user stored in a member database.

In contrast to Ratayczak, the present claims call for the use of a mobile communication terminal number corresponding to an identifier of a user stored in a member database and connection to the mobile terminal of the member by using the mobile terminal number. The applied references, in combination, fail to teach or suggest first identifying the user by comparing a first password, supplying a mobile communication terminal number corresponding to an identifier of a user stored in a member database, and then connecting to a mobile terminal of the member through a

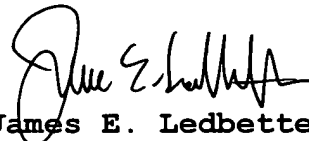
communication line by using the mobile communication terminal number, to receive and verify a second password.

Accordingly, the applied references, alone or together, fail to disclose or suggest retrieval of a mobile terminal call number or a communication circuit as defined in claim 11, step (d) or in claim 13, lines 11-13.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



James E. Ledbetter
Registration No. 28,732

Date: June 30, 2004
JEL/att
Attorney Docket No. JEL 31225
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200